[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request Extension from OMB of One Current Public Collection of Information: Pipeline Operator Security Information

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0055, abstracted below that we will submit to OMB for an extension in compliance with the Paperwork Reduction Act (PRA). On May 26, 2021, OMB approved TSA's request for an emergency revision of this collection to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. TSA is now seeking to renew the collection as it expires on November 30, 2021. The ICR describes the nature of the information collection and its expected burden. Specifically, the collection involves the submission of data concerning pipeline security incidents, appointment of cybersecurity coordinators, and coordinators' contact information.

DATES: Send your comments by **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Comments may be e-mailed to TSAPRA@tsa.dhs.gov or delivered to the TSA PRA Officer, Information Technology (IT), TSA-11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6011.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh at the above address, or by telephone (571) 227-2062.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation will be available at http://www.reginfo.gov upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to--

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

OMB Control Number 1652-0055; Pipeline Operator Security Information. In addition to TSA's broad responsibility and authority for "security in all modes of transportation … including security responsibilities … over modes of transportation [,]" *see* 49 U.S.C. 114, TSA is required to issue recommendations for pipeline security measures and conduct inspections to assess implementation of the recommendations. *See* sec. 1557 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53 (August 3, 2007). Consistent with these requirements, TSA produced Pipeline Security Guidelines in December 2010 and 2011, with an update published in April 2021.

As the lead Federal agency for pipeline security and consistent with its statutory authorities, TSA needs to be notified of all (1) incidents that may indicate a deliberate attempt to disrupt pipeline operations and (2) activities that could be precursors to such an attempt. The Pipeline Security Guidelines encourage pipeline operators to notify the Transportation Security Operations Center (TSOC) via phone or email as soon as possible if any of the following incidents occurs or if there is other reason to believe that a terrorist incident may be planned or may have occurred:

- Explosions or fires of a suspicious nature affecting pipeline systems, facilities, or assets.
- Actual or suspected attacks on pipeline systems, facilities, or assets.
- Bomb threats or weapons of mass destruction threats to pipeline systems, facilities, or assets.
- Theft of pipeline company vehicles, uniforms, or employee credentials.
- Suspicious persons or vehicles around pipeline systems, facilities, assets, or right-of-way.
- Suspicious photography or possible surveillance of pipeline systems, facilities, or assets.
- Suspicious phone calls from people asking about the vulnerabilities or security practices of a pipeline system, facility, or asset operation.
- Suspicious individuals applying for security-sensitive positions in the pipeline company.
- Theft or loss of Sensitive Security Information (SSI) (detailed pipeline maps, security plans, etc.).

When voluntarily contacting the TSOC, the Guidelines request pipeline operators to provide as much of the following information as possible:

- Name and contact information (email address, telephone number).

- The time and location of the incident, as specifically as possible.
- A description of the incident or activity involved.
- Who has been notified and what actions have been taken.
- The names and/or descriptions of persons involved or suspicious parties and license plates as appropriate.

On May 26, 2021, OMB approved TSA's request for an emergency revision of this information collection. *See* ICR Reference Number: 202105-1652-002. The revision was required as a result of the recent ransomware attack on one of the Nation's top pipeline supplies and other emerging threat information. TSA issued a Security Directive (SD) with requirements for TSA-specified critical pipeline owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities. The SD included two new information collections. TSA now requires all owner/operators subject to the SD's requirements to report cybersecurity incidents or potential cybersecurity incidents on their information and operational technology systems to the Cybersecurity & Infrastructure Security Agency (CISA) within 12 hours of discovery using the CISA Reporting System. In addition, the SD requires critical pipeline owner/operators to appoint cybersecurity coordinators and to provide contact information for the coordinators to TSA. To ensure that information reported pursuant to the SD is identifiable within the system, TSA requires these owners /operators to indicate that they are providing the information pursuant to the SD. TSA is now seeking renewal of this revised information collection for the maximum three-year approval period.

Using the CISA reporting system, TSA expects the mandatory reporting of pipeline cybersecurity incidents to CISA will occur 20 times per year for each pipeline owner/operator, and it will take approximately 2 hours to gather the appropriate information to submit each incident report. The potential burden to the public for this task is 100 x 20 x 2 hours = 4,000 hours.

TSA estimates that approximately 100 pipeline owner/operators will report their cybersecurity manager and alternate point of contact information. It will take the pipeline owner/operator approximately 30 minutes (0.50 hour) to do so, and the potential burden for this task is 100 x 0.50 hour = 50 hours.

For non-cybersecurity pipeline incidents, TSA expects voluntary reporting of pipeline security incidents will occur on an irregular basis. TSA estimates that approximately 32 incidents will be reported annually, requiring a maximum of 30 minutes (0.50 hour) to collect, review, and submit event information. The potential burden to the public for this task is estimated to be 16 hours. Therefore, the total hour burden to the public for this information collection request is estimated to be 4,000 hours + 50 hours + 16 hours = 4,066 hours annually.

Dated: June 24, 2021.

Christina A. Walsh,

TSA Paperwork Reduction Act Officer,

Information Technology.

[FR Doc. 2021-13885 Filed: 6/29/2021 8:45 am; Publication Date: 6/30/2021]